MUSKOKA ALGONQUIN HEALTHCARE	**Policy/Procedure Name:**	**Privacy Policy**
Manual: Administrative	**Number:**	
Section: Risk Management	**Effective Date:**	01 Nov 2004
Pages: 1 of 13	**Revision Date:**	01 Dec 2012

Purpose

The purpose of this policy is to assert Muskoka Algonquin Healthcare's commitment to the protection of personal health information ("PHI") from unauthorized collection, access, use, or disclosure, and protection of PHI from theft or loss. This policy addresses the appropriate collection, use and disclosure of PHI, the patient's right to limit access to his/her medical record, and the secure disposal of PHI when it is no longer required.

Scope

The policy pertains to all staff members and physicians at Muskoka Algonquin Healthcare (MAHC).

Policy Statement

Muskoka Algonquin Healthcare has a legal responsibility to ensure all personal health information (PHI) and personal information (PI) in its possession, power or control is kept in strictest of confidence and disclosed in accordance with this Policy, and applicable laws. All information collected, used and disclosed by the hospital or its staff shall be treated in a manner that accords with the *Personal Health Information Protection Act* ("PHIPA") and the *Freedom of Information and Privacy Protection Act* ("FIPPA") as set out below.

Definitions

Personal Health Information Protection Act ("PHIPA")

The PHIPA was enacted November 1, 2004 and outlines privacy policies and practices for health information custodians in the province of Ontario. The purposes of the PHIPA are as follows:

- To establish regulations for the collection, use and disclosure of personal health information in a manner that protects the confidentiality of the information and the privacy of the individuals in question.
- To provide individuals with the right to access personal health information about themselves and to correct or amend such information, subject to certain exceptions.
- To provide independent review and resolution of personal health information complaints.

The Freedom of Information Privacy Protection Act (FIPPA)

On Dec 8, 2010, the Government of Ontario passed the *Broader Public Sector Accountability Act*, 2010 which brings hospitals under the ***FIPPA, effective*** January 1, 2012. FIPPA provides access to information controlled by public sector organizations in the interests of transparency, accountability and the exercise of democracy and protects the privacy of the individuals to whom

that information relates. All records created or which came into the hospital's custody or control after January 1, 2007 is subject to the Act.

Nothing in this Policy detracts from the Hospital's rights and responsibilities in respect of personal health information in its possession, power and/or control as set out in any law applicable in the province of Ontario including the *Public Hospitals Act, Child and Family Services Act*, *Health Protection and Promotion Act, Mental Health Act, and Regulated Health professions Act* and related regulations.

There will be instances where application of PHIPA or FIPPA conflicts with, or is inconsistent with, the statutory requirements of Ontario's own legislation. In these instances, the Hospital will seek advice from legal counsel to determine which legislative requirement is applicable/appropriate in the circumstances.

Definitions

'**Personal Health Information**' (PHI) refers to all health related information [as defined in the legislation & outlined below] that is linked to identifying information about an individual in either oral or recorded form. Health related information is defined in the legislation as information that relates to the:

Physical or mental health of an individual including the medical history of their family members;

- The health care provided to an individual
- The plan of service under the Long-Term Care Act, 1994;
- payments or eligibility for health care of an individual;
- donation of a body part or bodily substance of an individual or derived from testing or examination of any such body or bodily substance;
- An individual's health number;
- Identification of the hospital as the provider of health care to the individual or Substitute Decision Maker. (Bill 31, Personal Health Information Protection Act, section 4) [1]

'**Personal information'** is recorded information about an identifiable individual including:

- The individual's address, telephone number, fingerprints or blood type,
- Information about the individual's race, national or ethnic origin, colour, religion, age, sex, sexual orientation, marital or family status,
- Information about the individual's educational, medical, psychological, criminal, or employment history or information concerning his or her financial transactions,
- Any identifying number, symbol or other particular assigned to the individual,
- The individual's personal opinions or views except when they relate to someone else,

[1] Definition from the Protection of Personal Health Information policy

- Private or confidential correspondence sent to an institution by the individual, and replies to that correspondence that would reveal the contents of the original correspondence,
- The views or opinions of someone else about the individual, and
- The individual's name when it appears with other personal information about that individual or when disclosure of the name would reveal other personal information about that individual.

'**Identifying information'** is information that identifies an individual or for which it is reasonably foreseeable in the circumstances that it could be utilized, either alone or with other information, to identify an individual.

- Individuals have the right of access to their own PI and the right to request correction of that information
- Hospitals must maintain a PI Bank and document the official FIPPA requests for PI

'Privacy' is the right of an individual to control his or her own personal information. In other words, a person can determine how, when, and to what extent, they will share information with others. With respect to health information, the right of privacy includes a patient's right to know of, and exercise control over, any information about them.

'Confidential Information' is information of a sensitive nature in any format which is created or received by the hospital in the course of its business which is not otherwise available to the public and includes, but is not limited to, the following:

- Patient Information: Any information which could lead to the identification of a specific patient, or family member/significant other of a patient;
- Personal Information: Any information about an identifiable individual;
- Financial Information: Any information that would outline a person's salary or any unpublished financial information (e.g., suppliers, debtors, payroll);
- Human Resources Information: Any performance-related information, compensation, benefits, WCB, or occupational health information;
- Legal Information: Any information outlined in a legal document (e.g., contracts, agreements, disputes);
- Human Rights Information: Any information that is associated with an informal or formal human rights complaint, including an abuse or harassment complaint;
- Other Administrative Information: Any information used for administrative purposes (e.g., schedules, patient census, employee lists, patient lists, donor lists, etc.);
- Business Information: Any information related to the hospital's strategic initiatives (e.g., organizational restructuring, mergers, and outsourcing of business units).

Maintaining confidentiality is the obligation of staff and affiliates to protect information entrusted to them regardless of format; formats may include, but are not limited to verbal, written, and electronic.

'Staff' means the employees, privileged staff members, volunteers, directors, and anyone else under the control of the Hospital who has cause to deal with personal health information in the possession, power or control of the Hospital;

The Ten Privacy Principles

Principle #1: Accountability

Muskoka Algonquin Healthcare (MAHC) is responsible for information under in its possession, power or control, including information that has been transferred by the Hospital or its staff to a third party for processing. The Hospital shall take the necessary steps (by contract) to ensure that a comparable level of privacy protection attaches to any personal health information that is placed by the Hospital into the hands of a third party for any reason.

- Accountability for MAHC's compliance with the Policy rests with the Chief Executive Officer, although other individuals within MAHC are responsible for the day-to-day collection and processing of personal and health information. In addition, other individuals within MAHC are delegated to act on behalf of the Chief Executive Officer, as follows:
    - Privacy Officer
    - Manager, Health Information Services
- The Privacy Officer will be responsible for keeping up-to-date with legal privacy developments and with best practices within the hospital and healthcare industry.
- The Privacy Officer for the Hospital shall be indicated on the Hospital's organization chart. The PO is designated by MAHC to oversee its compliance with these principles is a matter of public record. The privacy officer can be contacted as follows:
    - Tel- (705) 789-0022, ext. 6001
    - E-mail- privacy@MAHC.ca
- MAHC will implement policies and practices to give effect to this policy, including

    A. Implementing procedures to protect personal health information.

    B. Establishing procedures to receive and respond to complaints and inquiries.

    C. Training staff and communicating to staff information about MAHC's privacy policies and practices.

    D. Developing information to explain MAHC's policies and procedures

    E. Determining an access to information process to respond in a timely manner to individual requests for access to their personal health information, personal information of records in the custody or control of the hospital.

Principle #2: Identifying Purposes for the Collection

At or before the time personal and/or personal health information is collected, MAHC will identify the purposes for collection. The primary purposes for collection is for the delivery of direct patient care, employment, the administration of the hospital and health care system, teaching, statistics, research and complying with legal and regulatory requirements.

- Identifying the purposes for which personal health or personal information is collected at or before the time of collection allows MAHC to determine the information it needs to collect to fulfill these purposes.
- The identified purposes are specified at or before the time of collection to the individual from whom the personal health information is collected. Depending upon the way in which the information is collected, this can be done orally or in writing. An admission, appointment form, employee record for example, may give notice of the purposes. A patient who presents for treatment is also giving implicit consent for the use of his or her personal health information for authorized purposes.
- When PHI or PI has been collected is to be used for a purpose not previously identified, the new purpose will be identified prior to use. Unless the new purpose is required by law, the consent of the individual is required before information can be used for that purpose.
- Persons collecting PHI/PI will be able to explain to individuals the purposes for which information is being collected.

Principle #3: Consent for the Collection, Use, and

MAHC will obtain implied or expressed consent before collecting, using or disclosing personal health information. When collecting, using and disclosing patient's personal health information for health care purposes, MAHC will rely on implied consent. If the purpose is something other than health care, expressed consent will be obtained from our patients. Exception: there are specified circumstances where we may collect, use or disclose personal health information without consent. MAHC will rely on implied consent, where appropriate, or obtain express consent from our patients when collecting, using or disclosing their personal health information, unless otherwise exempted by the Acts.

- MAHC will seek consent for the use or disclosure of this information at the time of collection, where implied consent is not applicable. In certain circumstances, consent with respect to use or disclosure may be sought after the information has been collected but before use (for example, when MAHC wants to use information for a purpose not previously identified).
- The principle requires "knowledge and consent". MAHC will make a reasonable effort to ensure that the individual is advised of the purposes for which the information will be used. To make the consent meaningful, the purposes will be stated in such a manner that the individual can reasonably understand how the information will be used or disclosed.

- MAHC will not, as a condition of the supply of a product or service, require an individual consent to the collection, use, or disclosure of information beyond that required to fulfill the explicitly specified and legitimate purposes.
- The form of consent (implied, expressed verbal or written) used by MAHC may vary. The Consent Decision tree (OHA toolkit) will be used to assist (appendix 1)
- In obtaining consent, the reasonable expectations of the individual are also relevant. MAHC can assume that an individual's request for treatment constitutes implied consent for specific purposes. On the other hand, an individual would not reasonably expect that personal health information given to MAHC would be given to a company selling health-care products.
- Individuals (patients or substitute decision-makers) can give consent in many ways. For example:
  - If you ask patients for personal health information to open a record and they answer your questions, you can infer their consent to the collection of their information. An admission or appointment form may be used to seek consent, collect information, and inform the individual of the use that will be made of the information. By completing the form, the individual is giving consent to the collection and the specified uses;
  - Consent may be given orally when information is collected over telephone; or,
  - Consent may be given at the time that individuals receive a service or treatment.

- An individual may withdraw consent at any time, subject to legal or contractual restrictions and reasonable notice. MAHC will inform the individual of the implications of such withdrawal.

Principle #4: Limiting Collection

MAHC will limit the amount and type of personal health and personal information collected to that which is necessary for the purpose(s) identified. All information will be collected by fair and lawful means in order to ensure that individuals are not misled or deceived about the purposes for which the information is being collected and the Hospital shall not collect personal health information indiscriminately.

Principle #5: Limiting Use, Disclosure, and Retention

Personal health or personal information will not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal health information and personal information will be retained only as long as necessary for the fulfillment of those purposes.

- If using personal information for a new purpose, MAHC will document this purpose.

- MAHC will develop guidelines and implement procedures with respect to the retention of personal health information. These guidelines will include minimum and maximum retention periods. Personal health information that has been used to make a decision about an individual will be retained long enough to all the individual access to the informant after the decision has been made. MAHC is subject to legislative requirements with respects to retention periods.
- Personal health information that is no longer required to fulfill the identifying purposes will be destroyed, erased, or made anonymous. MAHC will develop guidelines and implement procedures to govern the destruction of personal health information,

Principle #6: Accuracy

Personal health and personal information will be accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used.

- The extent to which personal health and personal information will be accurate, complete and up-to- date will depend upon the use of the information, taking into account the interests of the individual. Information will be sufficiently accurate, complete, and up-to- date to minimize the possibility that inappropriate information may be used to make a decision about the individual.
- MAHC will not routinely update personal health information or personal information unless such a process is necessary to fulfill the purposes for which the information was collected.
- Personal health information and personal information that is used on an on-going basis, including information that is disclosed to third parties, will generally be accurate and up-to-date unless limits to the requirement for accuracy are clearly set out.

Principle #7: Safeguards for Personal health information

Personal health and personal information will be protected by security safeguards.

The security safeguards will protect information against loss or theft, as well as unauthorized access, disclosure, copying, use, or modification. MAHC will protect personal health information regardless of the format in which it is held.

- The nature of the safeguards will vary depending on the sensitivity of the information that has been collected, the amount, distribution, and format of the information, and the method of storage.
- The methods of protection will include:
  i. Physical measures, for example, locked filing cabinets and restricted access to offices;
  ii. Organizational measures, for example, confidentiality agreements (appendix 1), limiting access on a 'need-to-know' basis, and

iii. Technological measures, for example, the use of passwords and access controls, encryption, and audits.

- MAHC will make its employees, volunteers and physicians aware of the importance of maintaining the confidentiality of personal health and personal information. As a condition of employment, all new MAHC employees/agents (e.g. employee, clinician, physician, allied health, volunteer, researcher, student, consultant, vendor, or contractor) must sign the MAHC Confidentiality Agreement.
- Care will be used in the disposal or destruction of personal health and personal information, to prevent unauthorized parties from gaining access to the information.

Principle # 8: Openness about Personal health and personal information Policies and Practices

MAHC will make readily available to individuals specific information about its policies and practices relating to the management of personal health information.

- MAHC will be open about its policies and practices with respect to the management of personal health information. Individuals will be able to acquire information about its policies and practices without unreasonable effort. This information will be made available in a form that is generally understandable.
- The information made available will include:

i. The name or title, and the address, of the Privacy Officer, who is accountable for MAHC's privacy policies and practices, and to whom complaints or inquiries can be forwarded;

ii. The means of gaining access to personal health information held by MAHC;

iii. A description of the type of personal health and personal information held by MAHC, including a general account of its use;

iv. A copy of any brochures or other information that explains MAHC's policies, standards, or codes, and;

v. What personal health or personal information is made available to related organizations.

- MAHC may make information on its policies and practices available in a variety of ways. For example, MAHC has posted a statement on information practices and may choose to make brochures available in high traffic patient areas (e.g. emergency room), mail information to its patients or provide online access.

Principle #9: Individual Access

Upon request, in accordance with PHIPA or FIPPA an individual will be informed of the existence, use, and disclosure of his or her personal health or personal information and will be

given access to that information. An individual will be able to challenge the accuracy and completeness of the information and have it amended as appropriate.

Note: In certain situations, MAHC may not be able to provide access to all the personal health or personal information it holds about an individual or records in its custody or control. Exceptions to the access requirement will be limited and specific. The reasons for denying access will be provided to the individual upon request. Exceptions may include information that is prohibitively costly to provide, information that contains references to other individuals, information that cannot be disclosed for legal, security, or commercial proprietary reasons, and information that is subject to solicitor-client or litigation privilege.

- Upon request, MAHC will inform an individual whether or not it holds personal health or personal information about the individual. MAHC will seek to indicate the source of this information and will allow the individual access to this information. However, MAHC may choose to make sensitive medical information available through a medical practitioner. In addition, MAHC will provide an account of the use that has been made or is being made of this information and an account of the third parties to which it has been disclosed.
- An individual will be required to provide sufficient information to permit MAHC to provide an account of the existence, use, and disclosure of personal health or personal information. The information provided will only be used for this purpose.
- In providing an account of third parties to which it has disclosed personal health or personal information about an individual, MAHC will attempt to be as specific as possible. When it is not possible to provide a list of the organizations to which it has actually disclosed information about an individual, MAHC will provide a list of the organizations to which it may have disclosed information about the individual.
- MAHC will respond to an individual's request to access his/her personal health or information within a reasonable time period and at minimal or no cost to the individual. The requested information will be provided or made available in a form that is generally understandable. Where copies of the information (e.g. health record) are requested, the usual fee for this service will apply.
- When an individual successfully demonstrates the inaccuracy or incompleteness of personal health or personal information, MAHC will amend the information as required. Depending upon the nature of the information challenged, amendment involves the correction, deletion, or addition of information. Where appropriate, the amended information will be transmitted to third parties having access to the information in question.
- When a challenge is not resolved to the satisfaction of the individual, MAHC will record the substance of the unresolved challenge. When appropriate, the existence of the unresolved challenge will be transmitted to third- parties having access to the information in question, when applicable.

Principle #10: Challenging Compliance with MAHC's Privacy Policies and Practices

An individual will be able to address a challenge concerning compliance with this policy to the Privacy & Access Officer or Chief Executive Officer of MAHC.

- MAHC will put procedures in place to receive and respond to complaints or inquiries about its policies and practices relating to the handling of personal health and personal information. The complaint procedures will be easily accessible and simple to use.
- MAHC will inform individuals who make inquiries or lodge complaints of the existence of relevant complaint procedures.
- MAHC will investigate all complaints. If a complaint is found to be justified, MAHC will take appropriate measures, including if necessary, amending its polices and practices.

Cross Reference

Management of Breach of Patient Privacy Policy
Access, Disclosure and Correction of Personal Health Information
Confidentiality of Information and Data Security

Notes

References / Relevant Legislation

Personal Health Information Protection Act ("PHIPA")
Freedom of Information and Privacy Protection Act ("FIPPA")
Sources of information that are referenced in the document and/or sources that provide further information related to the document content.

Provide a brief statement and link to the applicable legislation related to the document.

Appendices

Confidentiality Agreement

Appendix A
CONFIDENTIALITY AGREEMENT
GBHS / SBGHC / HDH / MAHC

This agreement is applicable to agents of GBHS/SBGHC/HDH/MAHC that the health care centre has established a contract relationship with which includes employees, physicians, clinicians, students, board members, community members of committees, volunteers, allied health and contracted services: management, support.

This agreement is applicable to agents of GBHS/SBGHC/HDH/MAHC that the health care centre has established a contract relationship with which includes employees, physicians, clinicians, students, board members, community members of committees, volunteers, allied health and contracted services: management, support.

During my association with GBHS/SBGHC/HDH/MAHC (the "Hospital"), I acknowledge that I will have access to;

(a) Confidential or proprietary information and material relating to the Hospital, its functions, agents and all persons affiliated with the Hospital; and/or

(b) Personal health information relating to the Hospital's patients/clients

As a condition of my association with GBHS/SBGHC/HDH/MAHC, I hereby agree and acknowledge the following:

1. I shall keep in strict confidence information of any nature related to the Hospital, its functions, employees, patients/clients and all persons affiliated with the Hospital. I agree not to access, disclose, copy, remove, use or give to any person or organization except in accordance with my Hospital duties, with the Hospitals specific written prior authorization or as permitted by law.

2. At all times, I shall respect the privacy of the Hospital's patients/clients, employees and all persons affiliated with the Hospital and shall only collect, use and/or disclose personal information relating to these individuals as required by the performance of my duties under the terms of my association with the Hospital and in accordance with the laws of Ontario and Canada.

3. I agree that I will not alter, destroy or interfere with any information provided to me/ or that I may have access to during the terms of my association with the Hospital except with authorization of the Hospital or otherwise agreed to as a part of my association with the Hospital and such is documented with appropriate authorization.

4. This confidentiality Agreement does not apply to information I previously and independently developed alone or with others prior to my association with the Hospital and that I can substantiate by written records or to information in the public domain.

5. I shall maintain the confidentiality and security of any systems User ID(s) and Password(s) that have been assigned to me by the Hospital to enable my access to any networks, applications and acknowledge that I am responsible for all actions taken and access carried out under them. I will not provide my access codes to anyone nor will I attempt to use those of others.

6. I shall only access, process and transmit confidential information using hardware, software and other GBHS/SBGHC/HDH/MAHC authorized equipment as required to by the duties of my position.

7. I will not or permit anyone else to read, copy, corrupt, disclose or destroy any of the data or systems information, programs or other information assets of GBHS/SBGHC/HDH/MAHC except where required for the performance of my duties and as authorized by GBHS/SBGHC/HDH/MAHC.

8. I acknowledge the Hospital issues policies and procedures that relate to the confidentiality, privacy and security of personal health information and the compliance with the terms of these policies are material term of my association with the hospital.

9. I further understand that it is my responsibility to familiarize myself with the terms of these policies and to keep myself informed of any changes to them or of any new policies and procedures issued to replace or supplement them. Should I have any questions about any policies including their applicability to me and their impact on the performance of my hospital duties, I may contact my manager or the office of the Chief Privacy Officer for answers.

10. I understand that the Hospital will conduct periodic audits to ensure compliance with this Confidentiality Agreement and will act on any issues of concern uncovered by an audit.

11. Regardless of any changes that may occur to my title, duties, status and/or other terms of my association with the Hospital, I understand and agree that the terms of this Confidentiality Agreement will continue to apply.

12. I understand and agree to abide by all the conditions outlined above. I further understand and agree this Confidentiality Agreement will remain in force when I no longer have an association with the Hospital.

13. I also understand that a breach of these conditions may result in disciplinary action up to and including termination of employment and/or association, loss of privileges, termination of a contract.

The following are the policies and procedures associated with this confidentiality agreement:

MAHC specific policies:

- *Privacy Policy*
- *Management of Breach of Patient Privacy Policy*

Last Reviewed Date: 03/14/2018 00:00:00	**Signing Authority:** Senior Leadership Team
Next Review Date: 03/14/2021 00:00:00	**Version:** 1.0
Disclaimer Message: A printed copy of this document may not reflect the current, electronic version in the MAHC Document Management System (DMS). Any copies of this document appearing in paper form should always be checked against electronic version prior to use.	
Date/Time Generated: Nov 08, 2018 15:21	**Generated By:** gbin\tammy.tkachuk

- *Access, Disclosure and Correction of Personal Health Information*
- *Confidentiality of Information and Data Security*

Definition:
Agent-any person representing the organization(s)

_____ _____

Signature Date

Last Reviewed Date: 03/14/2018 00:00:00	**Signing Authority:** Senior Leadership Team
Next Review Date: 03/14/2021 00:00:00	**Version:** 1.0
Disclaimer Message: A printed copy of this document may not reflect the current, electronic version in the MAHC Document Management System (DMS). Any copies of this document appearing in paper form should always be checked against electronic version prior to use.	
Date/Time Generated: Nov 08, 2018 15:21	**Generated By:** gbin\tammy.tkachuk